LAUS SEMPER JESU ET MARIAE

JM

THORNTON

IT Acceptable Use & Online E-safety Policy

Mission Statement

'To educate young people to meet the challenges of life courageously, to use their talents to the full and to live the values of Christ's Gospel'

This policy outlines our purpose in providing IT e-safety facilities and access to the internet and explains how the school is seeking to avoid the potential problems caused by unrestricted internet access.

1. Aims and Objectives

It is the duty of Thornton College to ensure that every Student in its care is safe; and the same principles apply to the digital world as apply to the real world. In the use of digital technology we aim to ensure that we keep children safe online, prevent cyber incidents and upgrade & maintain technology in cost-effective ways with recommendations to help meet the digital and technology standards. We also take the appropriate action to meet the cyber security standards and have implemented a Cyber Security Strategy. We acknowledge and embrace the evolving use of AI which is covered by our AI Policy.

Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our Students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy (for all staff, visitors and Students), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection & Safeguarding policy
- Behaviour Policy
- Staff Behaviour Policy;
- GDPR and Camera Use Policy
- Data Privacy Notice;
- Educational Visits Policy;

- PSHEE Policy; and
- BYOD Policy

At Thornton College, we understand the responsibility to educate our Students on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving Students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, Students, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff and governors;
- "parents" includes Students' carers and guardians; and
- "visitors" includes volunteers and anyone else who comes to the school.

This policy covers both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by Students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many Students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some Students, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by Students, in or out of school, will be dealt with under the school's Behaviour Policy and / or Child Protection & Safeguarding policy as is appropriate in the circumstances.

Students, staff and parents/carers are supported to understand the risks posed by:

- the CONTENT accessed by Students, that includes misinformation, disinformation (including fake news) and conspiracy theories.
- their CONDUCT on-line
- who they have CONTACT within the digital world
- COMMERCE - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the Child Protection & Safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Child Protection & Safeguarding policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Child Protection & Safeguarding policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its implementation and effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the DSL and Senior Leadership Team are adequately trained about online safety;

- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise & escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained. The Headteacher will ensure that the policy is implemented effectively.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at Thornton College. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Headteacher / Senior Leadership Team and IT Manager to achieve this. As such, in line with the Child Protection & Safeguarding policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the IT Manager and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.

3.4. IT Manager

The IT Manager will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

The school's IT Manager has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL.

3.5. Teaching and support staff

All staff are required to read, understand and agree to this policy, before accessing the school's systems and enforce it in accordance with direction from the DSL and the Headteacher / Senior Leadership Team as appropriate.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff are aware of the school policy for Online-Safety which sets out our expectations relating to:

- Creating a safer online learning environment,
- Giving everyone the skills, knowledge and understanding to help children stay safe on-line, question the information they are accessing and support the development of critical thinking,

- Inspiring safe and responsible use of mobile technologies, to combat behaviours on-line which may make Students vulnerable, including the sending of nude or semi-nude images.
- Use of camera equipment, including smart phones.
- What steps to take if there are concerns and where to go for help.
- Staff use of social media as set out in the Staff Code of Conduct.

Cyber-bullying by children, via texts, social media and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. School is aware of the risks posed by children in the online world; non-age-appropriate content linked to self-harm, suicide, grooming and radicalisation.

All staff understand expectations roles and responsibilities with regards to the online filtering and monitoring processes.

3.6. Students

Students are responsible for using the school IT systems in accordance with this Policy.

3.7. Parents and carers

Thornton College believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about Students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Online safety advice for parents is organised by the DSL.

4. Internet access in school

Providing access to the internet in school will raise educational standards and support the professional work of staff.

Teachers and students will have access to web sites world-wide (including museums and art galleries) offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DfE and receive up-to-date information.

The internet will also be used to enhance the school’s management information and business administration systems.

All staff (including teachers, technicians, learning support staff and boarding staff) and any other adults involved in supervising students accessing the internet, will be provided with the School IT Acceptable Use & E-safety Policy, and will have its importance explained to them.

Our school IT Acceptable Use & E-safety Policy will be available for parents and others to read on the website.

Ensuring Internet access is appropriate and safe

The internet is a communications medium and is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for students. Students in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that students do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our students are not exposed to unsuitable material:

- our internet access is purchased from Exponential-E and is filtered and monitored by our firewalls to prevent access to material inappropriate for students;
- Day students using the internet will normally be working in the classroom, during lesson time and during private study where they will be supervised by an adult (usually the class teacher) (all internet usage is monitored and restricted);
- staff will check that the sites pre-selected for student use are appropriate to the age and maturity of students;
- staff will be particularly vigilant when students are undertaking their own search and will check that the students are following the agreed search plan;
- students will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others;
- our 'Rules for Responsible internet Use' *(Shown at Appendix 1)* will be posted near computer systems.
- the IT Manager will monitor the effectiveness of internet access strategies;
- the IT Manager will ensure that occasional checks are made on files to monitor compliance with the school's IT Acceptable Use & E-safety Policy;
- methods to quantify and minimise the risk of students being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from our Internet Service Provider, our IT network service company and the DfE.
- Students will be trained in the safe use of the internet in their PSHEE lessons, form time, IT lessons and the Sixth Form Horizons programme.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. **The school cannot accept liability for the material accessed, or any consequences thereof**.

An important element of our 'Rules of Responsible internet Use' is that students will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a student is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on several levels. Responsibility for handling incidents involving students will be taken by the IT Manager & the Deputy Headteacher [DSL].

If one or more students discover (view) inappropriate material our first priority will be to give them appropriate support. The student's parents/guardians will be informed and will be given an explanation of the course of action the school has taken. The school aims to work with parents/guardians and students to resolve any issue.

If staff or students discover unsuitable sites, the IT Manager will be informed. The IT Manager will review and if necessary, block the website and report the URL (website address) and content to the Internet Service Provider; if it is thought that the material is illegal, after consultation with the ISP, the site will be referred to the internet Watch Foundation and the police. The IT Manager will also liaise with our IT network service company.

Using the Internet to enhance learning

Students will learn how to use a web browser and suitable web search engines. Staff and students will use the internet to find and evaluate information. Access to the internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that students learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the students:

- access to the internet may be by teacher demonstration;
- students may access teacher-prepared materials, rather than the open internet;
- students may be given a suitable web page or a single web site to access;
- students may be provided with lists of relevant and suitable web sites which they may access; older, more experienced, students may be allowed to undertake their own internet search having agreed a search plan with their teacher; students will be expected to observe the 'Rules of Responsible Internet Use' and will be informed that checks can and will be made on files held on the system and the sites they access.
- Students will be able to use their own electronic device to gain access to the internet using Thornton Wi-Fi, logging on using their own school network credentials. This must be adhered to and will allow their usage to be appropriately restricted and website use monitored.

Younger students accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the 'Rules of Responsible Internet Use' and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the students' minds as they monitor the students using the internet.

Using information from the Internet

We believe that, in order to use information from the internet effectively, it is important for students to develop an understanding of the nature of the internet and the information available. In particular, students should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it has copyright.

Students will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV; teachers will ensure that students are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium); when copying materials from the Web, students will be taught to observe copyright; students will be made aware that the composer of an e-mail or the author of a web page may not be the person claimed.

5. Filtering and Monitoring

In general:

Thornton College aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, Students, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's IT network through wifi or otherwise. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Behaviour Policy or the Behaviour Policy, as appropriate.

The IT Manager will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding Governor, the DSL and IT Manager will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content; this includes multi-lingual sites. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, the following: Harmful and inappropriate content including but not limited to, illegal or abusive material, child sexual exploitation content, content related to extremism and radicalisation, sexually explicit or violent content, or material that promotes self-harm or suicide, drug abuse, gambling material, malware/hacking material. If there is a good educational reason why a particular website, application, or form of content should not be blocked a Student should contact the relevant member of teaching staff, who will then contact the IT Manager and DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's IT network allowing individuals be identified. In line with the school's GDPR - Data Protection Policy and/or Privacy Notice, the IT Manager will monitor the logs daily. The DSL is sent live reports from the system. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the IT Manager and the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Child Protection & Safeguarding policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the IT Manager and the DSL if they believe that appropriate teaching materials are being blocked.

Students:

Students must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the IT Manager / DSL. Deliberate access to any inappropriate materials by a Student will be dealt with under the school's Behaviour Policy. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Students are expected to play their part in reducing the risk of viewing inappropriate material by obeying the ‘Rules of Responsible Internet Use’ which have been designed to help protect them from exposure to internet sites carrying offensive material. If students abuse the privileges of access to the internet, or use of e-mail facilities, by failing to follow the ‘Rules of Responsible Internet Use’, rules they have been taught, or failing to follow the agreed search plan, when given the privilege of undertaking their own internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/guardians. Teachers may also consider whether access to the internet may be denied for a period.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, Students should contact a member of the IT Manager for assistance.

6. Education and training

6.1 Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school’s expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school’s Online Safety procedures. These behaviours are summarised within this Policy which must be read and agreed before use of technologies in school.

All staff are expected to complete the Annual Online Safety through the National College. Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When Students use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

6.2 Students: the teaching of online safety

Online safety guidance will be given to Students on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our Students' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating Students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, Students are taught about their online safety responsibilities and to look after their own online safety. From Key Stage 2, pupils are taught, in an age-appropriate way, how to recognise unsafe online contact, including the risks of grooming and exploitation, and to understand the importance of reporting any concerns about themselves or others. Students can report concerns to the

DSL/ IT Manager and any member of staff at the school.

Educate Against Hate highlights approaches to take within schools in this important area, and the Pears Foundation reported earlier this year that the best way to tackle misinformation, disinformation and conspiracy amongst young people is through schools.

Senior students will receive e-safety training in Year 7 and regular updates during the preceding years. This will take place during IT lessons in Years 7-9 and in PSHEE in subsequent years, and the Sixth Form Horizon programme.

In the Horizon programme, PSHEE and form time, students in the Sixth Form will revisit the above and receive specific teaching regarding the appropriate use of IT (including Social Media)

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Anti Bullying / Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

7. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about Students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges annual discussion evenings for parents about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

8. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the BYOD Policy, Staff Behaviour Policy and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Thornton College are permitted to bring in personal devices for their own use. They may use such devices only during break-times and lunchtimes.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any Student nor to have any images, videos or other recording of any Student on their personal devices. Please read this in conjunction with Child Protection & Safeguarding Policy, Acceptable Use, Staff Code of Conduct and School Trips policies.

Students

Boarders must leave all personal devices in their respective Houses during the school day unless using in line with the school’s BYOD Policy.

All personal devices are brought in at the student’s own risk. All devices should require a password to be unlocked and this should never be divulged to any other student. The school does not take any responsibility for stolen, lost or damaged devices, including lost or corrupted data on these devices.

Please check with your homeowner's policy regarding coverage of personal electronic devices. The school is not responsible for any possible device charges that may be incurred during school- related use.

For Years 9-13: If students bring in mobile devices/tablets/laptops/chrome-books (e.g. for use during the journey to and from school), they will remain the responsibility of the student in case of loss or damage. Please refer to the BYOD policy.

For Years 7-8: If students bring in mobile phone devices they must be handed in to their form tutor, (these devices are locked in lockers within the form room) and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet via 4G, including smartwatches and other wearable technology. If students bring in tablets/laptops/chrome-books they will remain the responsibility of the student in case of loss or damage. Please refer to the BYOD policy.

The school has a bank of tablets which are used as a teaching and learning tool and Students are required to adhere to the IT Acceptable Use / Student BYOD Policy when using either a school tablet or any BYOD device for school work. In particular, the IT Acceptable Use / Student BYOD Policy requires Students to ensure that their use of tablets for school work complies with this policy and the IT Acceptable Use / Student BYOD Policy prohibits Students from using tablets for non-school related activities during the school day.

Any School mobile technologies made available for Student use by Thornton College [including laptops, tablets, cameras, etc.] are stored in a locked cupboard. Access is available via Head of IT / the IT Manager / Head of Art / the Housemistress. Members of staff should sign devices out and in before and after each use by a Student.

The 'Thornton Wi-Fi' network must be used to sign in; this network is monitored and filtered at all times. Any attempt to bypass the network, including the use of Virtual Private Networks (VPN's) or Proxies is strictly prohibited and will result in confiscation of the device. All BYOD devices are to be registered with the IT Manager before use in line with the BYOD Policy. All students must follow the acceptable usage instructions as detailed below.

Acceptable Use of Electronic Devices

An electronic device is defined as any device that enables staff and students to connect to the internet or other electronic devices with mobile (3G/4G), Wi-Fi or Bluetooth networks. (E.g. tablets, phones, PDA, laptop etc.) The use of BYOD is covered by the BYOD Policy

Boarders have their own Acceptable Use of Technology in Boarding [Appendix 3]

Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by Students will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by Students for medical purposes or as an adjustment to assist Students who have disabilities or special educational needs. Where a Student needs to use a mobile device for such purposes, the Student's parents or carers should arrange a meeting with the SENCo or their Head of Year [HOY] to agree how the school can appropriately support such use. The SENCo/HOY will then inform the Student's teachers and other relevant members of staff about how the Student will use the device at school.

Using phones outside of class or without teacher permission

Students are not allowed to have their phones out during the school day without the teachers permission. Please refer to the behaviour ladder for sanctions.

Sixth Form students **may** use their devices for personal use outside of lessons. This includes making and receiving calls.

Visitor ICT & Wi-Fi

Visitors can use the Guest Wi-Fi available. A password will be made available to them upon request. They will be asked to read the Visitor IT & Wi-Fi Protocol *(Appendix 2).* Visitors may be given access to a restricted area on the network, governed by a password. No access will be given to databases, staff, or student areas.

9. Online Communications

Internet access and home/school links

Parents will be informed on MSP that students are provided with internet access as part of their lessons or during private study times. We will keep parents in touch with future ICT developments by email or letter.

Staff

Any digital communication between staff and Students or parents / carers must be professional in tone and content. Under no circumstances may staff contact a Student or recent alumni (i.e. Students over the age of 18, until they reach the age of 21) using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with Students and recent alumni. Under no circumstances may staff contact a Student or recent alumni using a personal telephone number, email address, or other messaging system nor should Students and recent alumni until the age of 21 be added as social network 'friends' or similar. Current parents must only be contacted using the school's emailing system and personal details should never be shared.

Staff must immediately report to the DSL / Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Manager.

Staff may wish to access the internet for many purposes. Examples are:-

- to develop their teaching resources and / or to build their knowledge for supporting their teaching and learning.
- to communicate electronically with a range of individuals linked to education and the school to support the daily operation of the school.
- to receive educational publications or information of relevance to teaching and learning and / or the management of the school.
- to use "live" material on the internet directly in their teaching material.
- to use the internet for private purposes at appropriate times, provided it does not hinder any member of staff from fulfilling their duties.
- residential boarding staff may use the school network for personal use when off duty.

Staff using the internet must never:

- access information that is offensive and/ or inappropriate for use in a school, and/or save it to any medium.
- send offensive material through the school's internal or external email facilities.

- use the school's facilities to print out excessive material for private purposes.
- disclose any login username or password to anyone.
- leave their computers logged in.
- disclose any information regarding students or staff to any other person outside the school; all such information should be regarded as confidential and is covered by the Data Protection Act of 2018 as well as the school's GDPR Policy.
- download, use or upload any material from the internet, which is the copyright of others, unless an agreement has been entered into. *Please note: Any such agreements should go through the Headteacher or Bursar.*

Staff must pay due care to the following:

- Contact from a member of staff with parents should happen via the school e-mail only. All members of staff have a school e-mail address and this should be the one they use to correspond with parents.
- Members of staff should not use their private e-mail addresses to contact parents or students. A disclaimer must be attached to the signature of every e-mail sent by a member of staff.
- Contact with parents may be carried out by alternatively using Isams or MS Teams.

Students

All Students are issued with their own personal school email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work / assignments / research / projects. Students should be aware that email communications through the school network and school email addresses are monitored.

Students are not permitted to have staff private e-mail address contact but may contact staff through their school email address at the behest of teacher. Communication with students will also be carried out using MS Teams. In the Sixth Form, X (formally Twitter) can be used as a communication tool, i.e subjects may have an X account to share relevant articles. Any posts, comments or 'Tweets' used must be appropriate and not violate the staff conduct policy.

Using e-mail

Students from Year 5 onwards will learn how to use an e-mail application and be taught e-mail conventions. Staff and students will begin to use internal e-mail to communicate with others, to request information and to share information. Years 3 & 4 use the school email only for communication with teachers during a 'working from home' scenario.

It is important that communications with people and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained.

Therefore:

- students will only be allowed to use e-mail once they have been taught the 'Rules of Responsible Internet Use' and the reasons for these rules.
- teachers will endeavour to ensure that these rules remain uppermost in the students' minds as they monitor students using e-mail;
- students all have their own school email account;

- students may send e-mail as part of planned lessons;
- students may not access or send personal e-mail during lessons;
- students will have the e-mail messages they compose as part of planned lessons checked by a member of staff before sending them;
- the forwarding of chain letters will not be permitted;
- students will not be permitted to use e-mail at school to arrange to meet someone outside school hours or for personal use.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, Students should contact the IT Manager for assistance.

We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons. The IT Manager will ensure virus protection is kept up to date (this is automated), will stay updated with IT news developments, and work with the IT Network Service Company to ensure system security strategies are relevant to protect the integrity of the network. These are reviewed regularly and improved as and when necessary. This may include restrictions on e-mail attachments and downloads.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the IT Manager / DSL.

10. Use of social media

Staff

Staff must not access social networking sites, any website or personal email which is unconnected with school work or business from school devices whilst teaching / in front of Students. Such access may only be made from staff members' own devices or whilst in the staff room or staff-only areas of school.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Behaviour Policy.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Thornton College into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Behaviour Policy or Child Protection and Safeguarding Policy.

Students

The school expects Students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by Students vary seriously and incidents will be dealt with under the Behaviour, Child Protection & Safeguarding and Anti-Bullying policies as appropriate].

11. Data protection

Please refer to the GDPR & Camera Use policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and Students are expected to save all data relating to their work to their school laptop / PC or to the One Drive in Microsoft Office 365.

Staff devices should be encrypted if any data or passwords are stored on them. The school discourages the use of removable media but expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or Students should be stored on personal memory sticks, but instead stored in the cloud on One Drive or within iSams, Evolve or CPOMS.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager in accordance with the GPDR & Camera Use Policy and IT Acceptable Use Policy. Reference should be made to the Cyber Security Strategy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

12. Password security

Students and staff have individual school network logins and storage folders on the server. Staff and Students are regularly reminded of the need for password security.

All Students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers),
- not write passwords down; and
- not share passwords with other Students or staff.

Passwords for staff are changed every 91 days.

13. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and Students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and Students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate Students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

Please refer to the GDPR & Camera Use Policy for further information.

14. Artificial Intelligence

Any usage by Students of generative AI tools such as ChatGPT/Copilot is only permitted in the circumstances outlined in our Artificial Intelligence Policy, and subject to any conditions imposed by that policy.

In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, Students should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff.

15. Misuse

Thornton College will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity, they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any Student who misuses technology to bully, harass or abuse another Student in line with our Child Protection and Safeguarding and Behaviour policies.

16. Security of Network and Data

The School recognises the potential of a Cyber Attack and is covered by the school's Cyber Security Strategy. To mitigate this risk the school takes the following steps:

- Anti-virus protection is in place.
- An External Vulnerability Scan is run on a periodic basis and any vulnerabilities are addressed where possible.
- Staff permissions in Management Information Systems are appropriate and reviewed regularly.
- Past staff and students accounts are disabled upon leaving the college.
- Regular automatically enforced password changes are implemented to all staff periodically.
- Two factor authentication is enabled for all cloud-based systems.
- Updates/patches are actioned promptly across the network to include but not limited to:
    - Firewalls
    - Desktop Computers & Operating Systems
    - Backup Software
    - Filtering and Monitoring Software
    - Data Storage
    - Server Infrastructure
- Staff are advised to ensure that their passwords are complex, meet password complexity requirements and are kept secure.
- USB sticks are not to be used on the network – One Drive is preferred to prevent virus

infection and potential data leaks.

- All staff are trained using the following link: – https://youtu.be/pP2VKWSagE0
- Staff iPads are set to six-digit pin entries and the lock screen engages quickly for safety. iPads are not left accessible to students or other staff.
- Staff refrain from ticking any boxes in systems to ensure that verification codes are saved for several days.
- Lock screens on PCs are actioned when staff leave their desks. Staff room PCs are logged out after use.
- Encryption of sensitive business documents is in place.
- Staff have been trained and are on alert for suspicious phishing emails.
- Cyber-attack insurance protection is in place with CFC Underwriting Limited.

All this should be read concurrently with our GDPR Policy.

17. Complaints

As with all issues of safety at Thornton College, if a member of staff, a Student or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Deputy Head/DSL in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Child Protection and Safeguarding policy and reported to the school's DSL, Ms Tracey Wilks, in accordance with the school's Child Protection & Safeguarding Policy.

This information is available for all students and parents on MSP.

Rules for Responsible Internet Use

The school has installed computers with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will only access the computer system with my own username and password;
- I will not access other people's files;
- I will only bring in memory sticks or CDs from outside school to use on the school computers with permission from the ICT Teacher or Technician.
- I will not violate copyright laws.
- I will not use other people’s passwords or accounts.
- I will be mindful when using limited resources including printer ink and paper.

Using the Internet:

- I will ask permission from a teacher before using the Internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other students and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.
- I will not download music from the Internet or store my music on school computers.
- I will not give out the personal details of others.
- I will not upload/send photographs of myself or anyone at the school.

Using e-mail:

- I will check my personal e-mail only during scheduled lunch time or boarding house sessions;
- I will immediately report any unpleasant messages sent to me because this will help protect other students and myself;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or people my teacher has approved;
- I will only send an e-mail from a lesson when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number to people I don't know.

Appendix 2

Visitor IT & Wi-Fi Protocol

Thornton College's IT network has been set up to ensure a high degree of security to ensure that Students are protected as far as is reasonably possible from the threats associated with ICT. We currently use a web-filtering system which is designed specifically to protect schools. Any access to the web will go via this system.

As a visitor to Thornton College, you are welcome to use the school's wireless connections that are located around the school, on the following conditions:

1. You should login using the Guest Wi-Fi with a wireless key provided to access the wireless connection. This must be destroyed once you leave school and should not be passed on to any other user; it will not be passed on to any other person but will be for your sole use whilst you are visiting the school. Passwords to this area are changed regularly.
2. Ideally, you will use your own hardware device
3. If you do use the school's hardware, then you will log out when you are away from the machine, being ever vigilant of the security of the network.
4. You are responsible for protecting your own property.
5. The school will not be held responsible for damage to your property whilst on the school site.
6. You must never deliberately access information that is offensive and/ or inappropriate for use in a school, and/or save it to any external drive or cloud facility, neither on a school workstation or laptop.
7. You must not send offensive material through the school's internal or external email facilities.
8. You may not use the school's facilities to print out excessive material for private purposes.
9. You understand that you will not be able to access certain social networking sites.
10. You understand that the websites available will be monitored by the firewall system and searches for particular information will be visible by the Executive Team.
11. You will not contact any Students by e-mail or exchange any personal contact information with them.

Appendix 3

ACCEPTABLE USE OF TECHNOLOGY IN BOARDING AGREEMENT

2024-25

The boarding house encourages the use of technology to facilitate communication between boarding students and their family and friends. The school notes the potential social benefits of technology use but is also aware of the downsides and potential for misuse. Boarders are advised on positive ways to use technology and must avoid inappropriate use. Boarders are required to use their technology in accordance with the rules outlined in the Acceptable Use of Technology in Boarding Policy.

PERMITTED USES

Boarding students have access to their mobile devices as well as the computers available to them in ICT1 after school. The boarding house provides time in the evenings, in addition to study, between 16:20 – 17:30 for boarders to use the computers if needed for homework and studying. Boarders are required to hand in ALL devices every evening, to be stored in the locked boarding office overnight. Timings for device hand ins are dependent on the school year of each boarder. Year 11 and above do not need to hand in their phone on the weekend unless parents request otherwise, or unless Boarding Staff believe an alternative arrangement should be in place. Sixth Form (years 12 and 13) can always have their phones with them, unless requested otherwise by parents, or unless Boarding Staff believe an alternative arrangement should be in place.

PROHIBITED USES

School computers and mobile devices must not knowingly be used to:

- Send or receive material that is, or may be interpreted to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive or excessively personal.
- Send or receive material which harasses or promotes hatred or discrimination against any person or group of people
- Send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity
- Perform any activity using an anonymous or misleading identity
- Engage in any other illegal or inappropriate activity

IN ADDITION TO THIS

- No student may photograph or film other individuals without their consent
- No student may record a person's voice without their consent

SOCIAL MEDIA

Information boarders provide, and statements they make, on social media sites may impact on them and have significant consequences. Once information is put online, it is part of a permanent online record, even if someone attempts to remove it later.

All boarders are responsible for their words and actions. It is their responsibility to ensure that the posts made online are appropriate. If in doubt, do not post!

Boarders are not permitted to:

- Post photos of staff on social media.
- Post pictures or videos of other students without their explicit permission.
- Use the school's logo/school and boarding house name or create a school branded account for personal use which could be interpreted as representing the school.
- Contribute anything to social media which could bring staff, other students or the school into disrepute- for example, offensive blogs and photos.
- Invite staff members to join your personal social media site.
- Engage in discrimination, harassment or bullying of other students, staff and parents.
- Engage in any conduct that would not be acceptable in school/boarding house- see behaviour ladders.

WATCHING TV- IN BOARDING COMMON AREAS/ ON OWN DEVICES

Boarders are not permitted to:

- Watch any tv programmes/movies that are not their age rating. If unsure, please find a member of boarding staff.
- Listen to any music in the common areas/in boarding rooms that have explicit content**.**

Prep boarders are not permitted to use YouTube, unless supervised by a member of boarding staff (for example, for an activity).

Student Signature: ____________________________________

Housemistress Signature: ____________________________________

Parent signature: ____________________________________

Head of Boarding Signature: ____________________________________

Date: ____________________________________

Appendix 4

Thornton College – Bring Your Own Device (BYOD) Policy

Purpose

Thornton College is committed to providing a technology-rich learning environment that empowers students to be creative, collaborative, and independent learners. The purpose of this Bring Your Own Device (BYOD) policy is to set out clear expectations for the use of personal iPads/tablets, laptops or Chromebooks in class. The aim is to enhance teaching and learning while ensuring the safety, security, and well-being of all students, safeguarding users whilst protecting the integrity of the school's IT infrastructure.

At Thornton College, we believe that teaching students to be responsible digital citizens is as important as teaching them to use technology. All students participating in the BYOD programme are expected to demonstrate positive digital behaviour in line with the values of the school.

Scope

The policy applies to all students using personal electronic devices such as laptops or iPads on school premises during school hours, please see the *acceptable use of technology in boarding agreement* for information related to BYOD outside of the school day.

This is a rolling policy commencing September 2025 which takes into account parental feedback, and which will take the following format:

Years 7-8 will be permitted to bring a personal device (e.g. iPad/laptop) for educational use in school. They are not permitted to use any other type of device, including smartphones, and these will be securely stored in lockable storage by the form tutor at the beginning of the school day, for collection at the end of the school day.

Years 9-13 will be permitted to bring a personal device (including a smartphone) for educational use in school.

Conditions of Use

Educational Use Only: devices must be used only for learning purposes during lessons. Teachers will direct when and how devices may be used. Students must follow all instructions regarding device use.

Digital Footprint Awareness

Students should understand that their online actions are permanent and traceable. They are encouraged to build a positive digital footprint that reflects integrity and respect.

Educational Integration

Digital citizenship principles are integrated into the curriculum through:

- PSHE lessons
- ICT and computing classes
- Assemblies and workshops
- Tutor time discussion, including online safety campaigns

Students are expected to:

- Respect others online: Communicate kindly and respectfully in all digital interactions.
- Protect personal information: Avoid sharing passwords, addresses, or other sensitive data.
- Think critically: Evaluate the credibility of online sources and avoid spreading misinformation.
- Act ethically: Avoid plagiarism, respect copyright laws, and give credit when using others' work.
- Report concerns: Inform a teacher or trusted adult if they encounter cyberbullying, inappropriate content, or suspicious activity.

- Students must not:

- Use devices for gaming, social media, messaging, or streaming unless explicitly authorised.
- Record, photograph, or video others without explicit consent.

- Use devices to cheat, plagiarise, or engage in academic dishonesty.
- Attempt to bypass school network filters or access restricted content.
- Engage in cyberbullying, harassment, or any form of online abuse.
- Impersonate others or create false identities online.
- Use offensive, discriminatory, or threatening language or behaviour online.

Devices must arrive at school fully charged each day, charging during school hours is not guaranteed and should not be relied upon. Additionally, only plugs that have been PAT tested within school are permitted for use. Students are expected to maintain their device in working order, including updated security measures. Students are responsible for the physical care and safekeeping of their devices.

Eligible Devices
Students may bring the following types of devices for educational use:
iPads/tablets (Wi-Fi models only preferred), Windows or MacOS laptops, Chromebooks

- Requirements:
  - Wi-Fi capability
  - Up-to-date operating system.
  - Ability to run required educational apps (e.g., Office 365).

Not permitted:

- In Years 7-8: smartphones, smartwatches, handheld gaming consoles, or any other device with mobile data capability.
- In Years 9-13: students are permitted to use a smartphone for educational purposes only, as approved by a teacher. Smartwatches, handheld gaming consoles, or any other device with mobile data capability are not permitted.

Network Access
Students must connect only to the school's secure Wi-Fi network. Internet access is filtered and monitored to ensure safe usage and web filtering is used to block inappropriate or harmful content. Connecting to Wi-Fi enables firewall protection to prevent external threats and intrusion detection systems to monitor for suspicious activity.
Use of mobile hotspots, VPNs, or personal data connections is strictly prohibited and any attempt to bypass the Wi-Fi network and filters will be treated as a serious breach of policy.
Device Security
The school takes cybersecurity very seriously. Devices brought into school should comply with all other school policies (notably the school's IT acceptable use policy, and data protection policy). Suitable virus protection should be installed and updated; scanning devices regularly.
Students are expected to use strong passwords or biometric authentication (Face ID, fingerprint), enable auto-lock and encryption features.
Devices must not be:

- Jailbroken, rooted, or otherwise modified to bypass manufacturer security
- Shared with other students

Data Protection
Students must not store sensitive personal data (e.g., medical, financial) on their devices. Schoolwork should be saved to cloud-based platforms (e.g., OneDrive, Teams) with secure login credentials. Thornton College is not responsible for data loss or corruption on personal devices.
Physical Security
Devices must be clearly labelled with the student's name. Devices should be stored in lockers or secure bags when not in use. The school accepts <u>no</u> liability for lost, stolen, or damaged devices.
Incident Reporting

Any security incident (e.g., lost device, suspected malware, inappropriate content) must be reported immediately to a teacher or IT staff. The school reserves the right to inspect a device if there is reasonable suspicion of policy violation, in accordance with safeguarding and privacy laws.

Support and Maintenance

Thornton College will provide limited technical assistance, such as help connecting to Wi-Fi or accessing school systems.

Students are responsible for maintaining their device in good working order, including:

- Regular software updates
- Virus/malware protection (where applicable)
- Physical care (e.g., protective cases)

Consequences for misuse

Breaches of this policy may result in:

Verbal warning and reminder of expectations
Confiscation of the device for the remainder of the school day
Temporary or permanent suspension of BYOD privileges
Parental contact and possible disciplinary action
Further sanctions as outlined in the Behaviour Policy

Parental acknowledgement and consent

Parents/guardians must:

- Review and sign the Thornton College BYOD Agreement Form with their child.
- Ensure their child understands the responsibilities and rules outlined in this policy.
- Support the school's decision-making around any disciplinary outcomes related to BYOD misuse.

Review and Updates

This policy will be reviewed annually, or as needed, by the Senior Leadership Team in consultation with IT Support and teaching staff.

For any questions regarding this policy, please contact Hayley Mallendane, Assistant Headteacher.

Thornton College BYOD Policy Agreement

Name: ____________________________ Form: ______________

I agree to the following rules in relation to BYOD in school:

- I will only use my own device when permission has been given by a member of staff.
- I will only use the school network to access the internet from my own device.
- I will not record, send on or store any pictures, video or sound of any other person without their express permission.
- I will ensure that my BYO device is always set to 'silent' when switched on.
- I will not use my device to download any materials that are not directly for school work-related purposes.
- I understand that the safety of my device and all associated passwords is my own responsibility.
- I understand that I am responsible for any accidental damage or loss of my own device and any cost of repairs or replacement for it.
- I understand that the school will only provide limited technical support for my device.
- I will only use the authorised external media and features available to me to transfer data and access the school's network.
- I have read and understood the BYOD Policy and agree to abide by its conditions. I understand that misuse of a device may lead to the device being confiscated for return to parents and that I may lose the privilege to bring a device into school in the future.

Pupil Name: I confirm that I have read and understood the BYOD Policy	**Date:** **Signed:**
Parent Name:	Signed:

Frequently Asked Questions (FAQs)

Q1: What types of devices are allowed under the BYOD policy?

Only **iPads/tablets** and **laptops (Windows or macOS)/Chromebooks** are permitted. Devices must be capable of connecting to the school's Wi-Fi.

Q2: What happens if a student forgets their device or it runs out of battery?

Students are expected to bring their device fully charged each day. If a device is forgotten or unusable, the student may be required to complete work using traditional methods or borrow a school device if available. Only PAT tested chargers can be used for electrical safety reasons.

Q3: Will the school provide technical support for personal devices?

The IT department will assist with **Wi-Fi connectivity issues only**. Students and families are responsible for maintaining and troubleshooting their own devices.

Q4: Is the school responsible for lost, stolen, or damaged devices?
No. Students are responsible for the care and security of their own devices. The school is not liable for any loss, theft, or damage.

Q5: Can students use their own internet (e.g., mobile data or hotspots)?
No. All devices must connect through the **Thornton College Wi-Fi network** to ensure safe and filtered internet access.

Q6: Are students allowed to install any apps they want?
Students may install apps for personal use, but **only school-approved apps** may be used during lessons. Inappropriate or distracting apps must not be accessed during school hours.

Q7: How does the school ensure internet safety on personal devices?
The school uses **content filtering, firewalls, and network monitoring** to block inappropriate content and detect suspicious activity. Students must also follow digital citizenship guidelines.

Q8: Can teachers see what students are doing on their devices?
Teachers and IT staff can monitor network activity and may request to inspect a device if there is a **reasonable suspicion of misuse**, in line with safeguarding policies.

Q9: What should a student do if they see or experience cyberbullying or inappropriate content?
They should report it immediately to a teacher, form tutor, or the safeguarding team. All reports are taken seriously and handled confidentially.